



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/896,090	06/29/2001	Amy H. Kang	5181-91900	9493

7590 12/17/2004

Robert C. Kowert
Conley, Rose, & Tayon, P.C.
P.O. Box 398
Austin, TX 78767

EXAMINER

OSMAN, RAMY M

ART UNIT	PAPER NUMBER
----------	--------------

2157

DATE MAILED: 12/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/896,090	KANG ET AL.	
	Examiner	Art Unit	
	Ramy M Osman	2157	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 June 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-70 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-70 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 29 June 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) . | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

On line 11, the limitation “for sending to the second node” is unclear. There is no mention of what is being sent, which renders the sentence as an incomplete sentence.

Line 19 uses unclear language which makes the limitation hard to understand which node is controlling access, the first or second nodes. Examiner assumes that the following is meant: ... the second node controls access to its resources by the first node.

3. Claims 3,20,27,40 rejected under 35 U.S.C. 112, second paragraph, as being indefinite.

The claim uses unclear language which makes the limitation hard to understand which node is controlling access, the first or second nodes. Examiner assumes that the following is meant: ... the second node controls access to its resources by the first node.

4. Claims 9 rejected under 35 U.S.C. 112, second paragraph, as being indefinite. The limitation “for sending to the second node” is unclear. There is no mention of what is being sent, which renders the sentence as an incomplete sentence.

Art Unit: 2157

5. Claims 1,26,49,51,56,58 rejected under 35 U.S.C. 112, second paragraph, as being indefinite. The limitation 'plugging in', and its variations, are being interpreted as an installed module which implements an authentication protocol. In regards to the Swift et al. reference, the 'plugged in' module is the challenge-response protocol module, as cited below. This is different from independent claims 14,37,63, because those claims explicitly state that the "pluggable modules are configured to be replaced to support different authentication types".

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. **Claims 1-9,12,13,26-32,35,36,49-53 and 56-60 rejected under 35 U.S.C. 102(e) as being unpatentable over Swift et al (US Patent No 6,377,691).**

8. In reference to claims 1,26,49,51,56,58, Swift teaches methods and systems comprising:

determining an authentication type to be used between a first node and a second node in a networked computer system (column 3 lines 30-67);

plugging in a first authentication protocol handler module on the first node for the determined authentication type, wherein the first authentication protocol handler module is

Art Unit: 2157

configured for use in generating authentication information for the first node for sending to the second node (column 3 lines 59-61);

plugging in a second authentication protocol handler module on the second node for the determined authentication type, wherein the second authentication protocol handler module is configured for use in determining if the first node is authentic using the first node authentication information (column 3 lines 61-63);

determining an access control model to be used by the second node in controlling access to resources of the second node by the first node (column 4 lines 1-25, Swift discloses using challenge-response to control access to resources); and

plugging in an access control context module for the determined access control model on the second node, wherein the access control context module is configured for use in controlling access to resources of the second node by the first node using the access control model (Summary).

9. In reference to claims 2, Swift teaches the method as recited in claim 1, further comprising loading the determined access control model (column 7 lines 20-30).

10. In reference to claims 3,27,52,59, Swift teaches the methods and systems as recited in claims 1,26,51,58 respectively, wherein the access control context module encapsulates information configured for use in controlling access to the resources of the second node by the first node (column 4 lines 1-3).

11. In reference to claims 4,28, Swift teaches the methods as recited in claims 1,26 respectively, wherein the first authentication protocol handler module includes a handle request method, wherein the second authentication protocol handler module includes a handle response

method, wherein the handle request method and handle response method are configured to exchange authentication information during an authentication process for the first node (column 3 line 55 – column 4 line 25).

12. In reference to claims 5,29, Swift teaches the methods as recited in claims 1,26 respectively, further comprising:

the second node sending a challenge to the first node, wherein the challenge is in accordance with the determined authentication type (column 4 lines 2-6);

the first authentication protocol handler module generating response data in response to the challenge, wherein the response data includes information for use in authenticating the first node (column 4 lines 5-11);

the first node sending the response data to the second node (column 4 lines 5-11); and

the second authentication protocol handler module authenticating the first node using the received response data (column 4 lines 11-25).

13. In reference to claims 6,30,50,57, Swift teaches the methods and systems as recited in claims 5,29,49,56 respectively, wherein said authenticating the first node using the received response data comprises:

the second authentication protocol handler module sending the received response data to a user repository, wherein the user repository comprises node information associated with one or more network nodes (column 7 lines 1-15); and

the user repository comparing the response data to the node information to authenticate the first node (column 7 lines 1-15).

Art Unit: 2157

14. In reference to claims 7,31, Swift teaches the method as recited in claims 1,26 respectively, further comprising;

authenticating the first node using the first authentication protocol handler module and the second authentication protocol handler module (column 4 lines 1-25);

the authenticated first node sending to the second node a request for access to a resource of the second node (column 4 lines 1-25); and

the access control context module determining if the first node has access permission to the resource in response to the request for access to the resource of the second node (column 4 lines 1-25).

15. In reference to claims 8,32,53,60, Swift teaches the methods and systems as recited in claims 7,31,51,58 respectively, further comprising:

if said determining determines the first node has access permission to the resource, allowing the first node to access the resource (column 4 lines 10-25); and

if said determining determines the first node does not have access permission to the resource, inhibiting the first node from accessing the resource (column 4 lines 10-25).

16. In reference to claims 9, Swift teaches the method as recited in claim 1, wherein the second authentication protocol handler module is further configured for use in generating authentication information for the second node for sending to the first node (column 4 lines 1-15); and

wherein the first authentication protocol handler module is further configured for use in determining if the second node is authentic using the second node authentication information (column 4 lines 1-15).

Art Unit: 2157

17. In reference to claims 12,35, Swift teaches the method as recited in claims 1,26 respectively, wherein networked computer system is a client- server system, wherein the first node is a client in the client-server system, and wherein the second node is a server in the client-server system (column 7 lines 14-45).

18. In reference to claims 13,36, Swift teaches the method as recited in claims 1,26 respectively, wherein the networked computer system is a peer-to-peer system, wherein the first node and the second node are peers in the peer-to- peer system (column 7 lines 14-45).

Claim Rejections - 35 USC § 103

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

20. **Claims 14-21,24,25,37-44,47,48 and 63-70 rejected under 35 U.S.C. 103(a) as being unpatentable over Swift et al (US Patent No 6,377,691) in view of Samar (1996 ACM 0-89791-829-0/96/03).**

21. In reference to claims 14,37,63, Swift teaches a method, system and carrier medium for authenticating nodes in a networked computer system, comprising:

a first node initiating a connection to a second node in the networked computer system (column 3 lines 55-67);

determining an authentication type to be used by the first node and the second node
(column 3 lines 30-67);

initializing a first authentication protocol handler on the first node for the determined
authentication type (column 3 line 55 – column 4 line 10);

initializing a second authentication protocol handler on the second node for the
determined authentication type (column 4 lines 1-25);

the second node sending a challenge to the first node, wherein the challenge is in
accordance with the determined authentication type (column 4 lines 1-45);

the first authentication protocol handler generating response data in response to the
challenge, wherein the response data includes information for use in authenticating the first node
(column 4 lines 1-45);

the first node sending the response data to the second node (column 4 lines 1-45); and
the second authentication protocol handler authenticating the first node using the received
response data (column 4 lines 1-45).

Swift fails to explicitly teach wherein the first authentication protocol handler and the
second authentication protocol handler are pluggable modules configured to be replaced to
support different authentication types. However, Samar discloses a variety of pluggable
authentication modules that can be used to replace a different authentication type in a system.

It would have been obvious for one of ordinary skill in the art to modify Swift by making
the first authentication protocol handler and the second authentication protocol handler pluggable
modules configured to be replaced to support different authentication types as per the teachings

Art Unit: 2157

of Samar so that a variety of pluggable authentication modules can be used to replace a different authentication type in a system.

22. In reference to claims 15,64, Swift teaches the method and carrier medium as recited in claims 14 and 63 respectively, wherein said authenticating the first node using the received response data comprises:

the second authentication protocol handler sending the received response data to a user repository, wherein the user repository comprises node information associated with one or more nodes (column 7 lines 1-15); and

the user repository comparing the response data to the node information to authenticate the first node (column 7 lines 1-15).

23. In reference to claims 16,65, Swift teaches the method and carrier medium as recited in claims 14,63 respectively, further comprising, if the first node is successfully authenticated:

determining an access control model to be used by the second node for the first node (Summary); and

initializing an access control context module for the determined access control model, wherein the access control context module is configured for use in controlling access to resources of the second node by the first node using the access control model (Summary).

24. In reference to claims 17,18,38,39,66,67, Swift teaches the method, system and carrier medium as recited in claims 16,37 and 65 respectively. Swift fails to explicitly teach wherein the access control context module is a pluggable module configured to be replaced to support different access control models; and wherein the access control context module is configured to support different pluggable access control models. However, Samar discloses a variety of

Art Unit: 2157

pluggable authentication modules that can be used to replace a different authentication type in a system.

It would have been obvious for one of ordinary skill in the art to modify Swift by making the first authentication protocol handler and the second authentication protocol handler pluggable modules configured to be replaced to support different authentication types as per the teachings of Samar so that a variety of pluggable authentication modules can be used to replace a different authentication type in a system.

25. In reference to claims 19, Swift teaches the method as recited in claim 16, further comprising loading the determined access control model (column 7 lines 20-30).

26. In reference to claims 20,40, Swift teaches the method and system as recited in claims 16,37 respectively, wherein the access control context module encapsulates information configured for use in controlling access to the resources of the second node by the first node (column 4 lines 1-3).

27. In reference to claims 21,68, Swift teaches the method and carrier medium as recited in claims 16 and 65 respectively, further comprising:

the first node sending to the second node a request for access to a resource of the second node (column 4 lines 1-25);

the access control context module determining if the first node has access permission to the resource (column 4 lines 1-25);

if said determining determines the first node has access permission to the resource, allowing the first node to access the resource (column 4 lines 1-25); and

if said determining determines the first node does not have access permission to

the resource, inhibiting the first node from accessing the resource (column 4 lines 1-25).

28. In reference to claims 24,47,69, Swift teaches the method, system and carrier medium as recited in claims 14,37,63 respectively, wherein networked computer system is a client-server system, wherein the first node is a client in the client-server system, and wherein the second node is a server in the client-server system (column 7 lines 14-45).

29. In reference to claims 25,48,70, Swift teaches the method, system and carrier medium as recited in claims 14,37,63 respectively, wherein the networked computer system is a peer-to-peer system, wherein the first node and the second node are peers in the peer-to-peer system (column 7 lines 14-45).

30. In reference to claims 41, Swift teaches the system as recited in claims 37, further comprising:

the second node sending a challenge to the first node, wherein the challenge is in accordance with the determined authentication type (column 4 lines 2-6); the first authentication protocol handler module generating response data in response to the challenge, wherein the response data includes information for use in authenticating the first node (column 4 lines 5-11); the first node sending the response data to the second node (column 4 lines 5-11); and the second authentication protocol handler module authenticating the first node using the received response data (column 4 lines 11-25).

31. In reference to claims 42, Swift teaches the system as recited in claims 41, wherein said authenticating the first node using the received response data comprises:

the second authentication protocol handler module sending the received response data to a user repository, wherein the user repository comprises node information associated with one or

Art Unit: 2157

more network nodes (column 7 lines 1-15); and the user repository comparing the response data to the node information to authenticate the first node (column 7 lines 1-15).

32. In reference to claims 43, Swift teaches the system as recited in claims 37, further comprising;

authenticating the first node using the first authentication protocol handler module and the second authentication protocol handler module (column 4 lines 1-25); the authenticated first node sending to the second node a request for access to a resource of the second node (column 4 lines 1-25); and the access control context module determining if the first node has access permission to the resource in response to the request for access to the resource of the second node (column 4 lines 1-25).

33. In reference to claims 44, Swift teaches the system as recited in claims 37, further comprising:

if said determining determines the first node has access permission to the resource, allowing the first node to access the resource (column 4 lines 10-25); and if said determining determines the first node does not have access permission to the resource, inhibiting the first node from accessing the resource (column 4 lines 10-25).

Art Unit: 2157

34. Claims 10,11,22,23,33,34,45,46,54,55,61,62 rejected under 35 U.S.C. 103(a) as being unpatentable over Swift et al (US Patent No 6,377,691) in view of Samar (1996 ACM 0-89791-829-0/96/03) in further view of O'Brien (US Patent No 6,351,776).

35. In reference to claims 10,11,22,23,33,34,45,46,54,55,61,62, Swift teaches the methods and systems as recited in claims 1,14,26,37,49,56 respectively. Swift fails to explicitly teach wherein the networked computer system is a messaging-based system; and wherein the networked computer system uses the Java Message Service (JMS) to support messaging between nodes in the network. However, O'Brien discloses authenticating users in a network environment which contains the well-known JMS to support messaging (column 9 lines 55-65, column 10 lines 20-40 and column 11 lines 1-45).

It would have been obvious for one of ordinary skill in the art to modify Swift by making the networked computer system a messaging-based system; and the networked computer system uses the Java Message Service (JMS) to support messaging between nodes in the network as per the teachings of O'Brien since JMS is well known in the art, and for the purpose of authenticating users in a network environment which contains the JMS to support messaging.

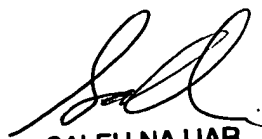
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ramy M Osman whose telephone number is (571) 272-4008. The examiner can normally be reached on M-F 9-5.

Art Unit: 2157

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on (571) 272-4001. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

RMO
December 8, 2004



SALEH NAJJAR
PRIMARY EXAMINER